

1/6

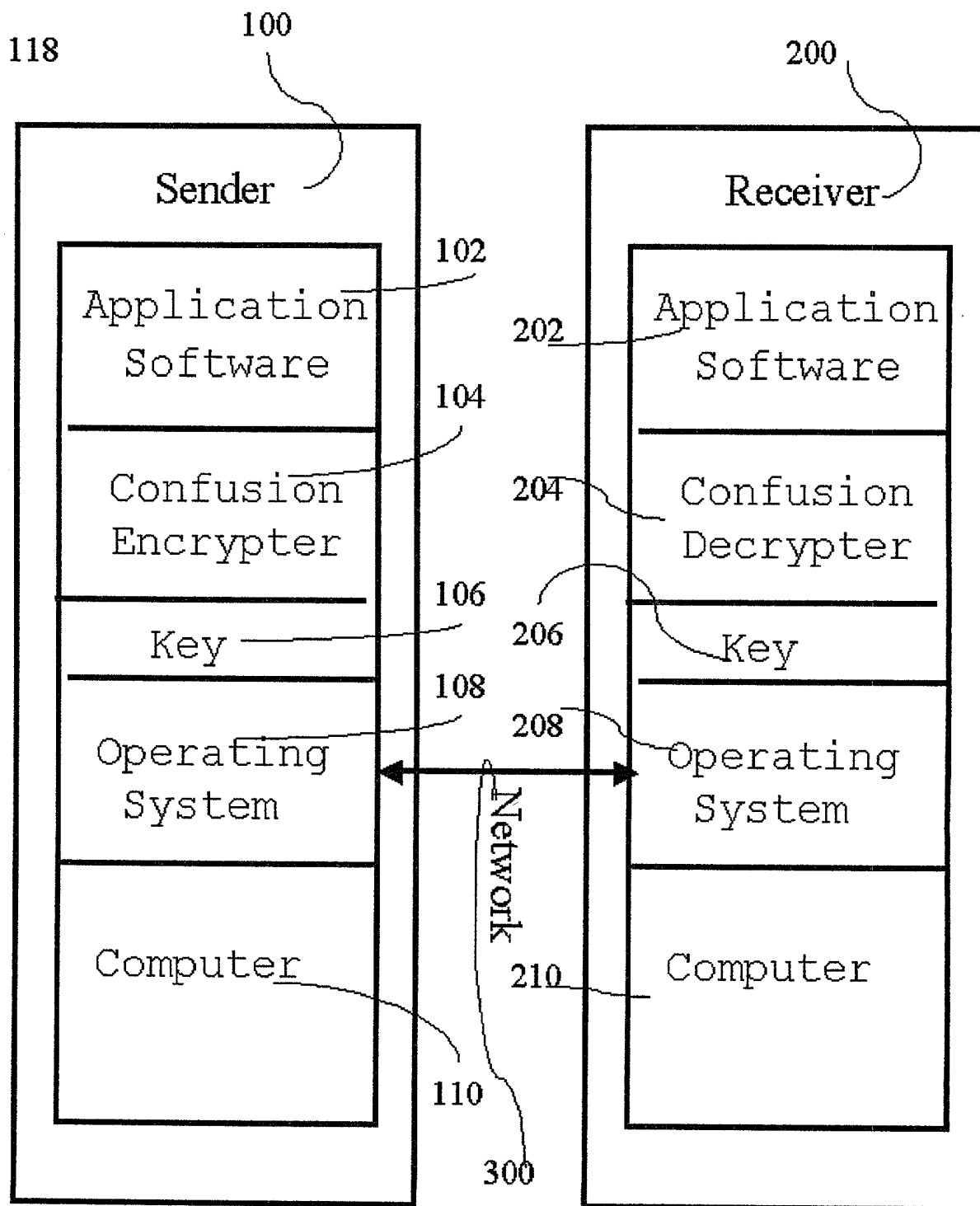


FIG.1

2/6

**Input:** A sequence of plaintext symbols  $p = \langle p_1, \dots, p_n \rangle$ , and the name of a file containing a key as described in K1-K6.

Let  $P_1$  be the set symbols in the plaintext, and let  $P_2 = P \cup (P_1 - T)$ .

Run  $g(n)$  to generate a random permutation  $h$  of  $\langle 1, \dots, n \rangle$  as described in K2.

Generate a random positive integer  $u$ .  
Run  $\text{lengths}(n, k, u) = \langle l_1, l_2, \dots, l_{(n+1)} \rangle$

Make pad sequences  $q_j$  for  $j=1, \dots, (n+1)$  as described in E4.

FIG.2

A

FOUO "00E88600

A

3/6

$C_1 = \langle q_1, p_{h(1)}, q_2, p_{h(2)}, \dots, q_n, p_{h(n)}, q_{(n+1)} \rangle$

Insert into  $c_1$ , starting at position  $s$ , a t-encoding of  $n$ , padded to length  $r$  with symbols in  $P_2$ . The result is a sequence  $c_2$  of length  $q = n + m + r$

Run the function  $\text{posn}_{\text{rotate}}(q) = s_q$   
 Rotate  $c_2$  circularly to the right by  $r_q$  symbol positions yielding  $c_3$ .  
 Insert into  $c_3$  at position  $s_q$  a t-encoding of  $r_q$  padded to length  $l_q$  with symbols from  $P_2$ .  
 The result is  $c_4$ .

Run the function  $\text{posn}_u(|c_4|) = s_u$ .  
 Insert into  $c_4$  at position  $s_u$  a t-encoding of  $u$  padded to length  $l_u$  with symbols from  $P_2$ .

Output the resulting ciphertext  $c$ .

FIG.3

10611-0033550

4/6

**Input:** A sequence  $c$  of ciphertext symbols, and the name of a file containing a key as described in K1 and K3-K6

Run the function  $\text{posn}_u(|c| - l_u) = s_u$ . Cut out from  $c$  a sequence  $e(u)$  of length  $l_u$  starting at position  $s_u$ , containing a t-encoding of  $u$ , leaving a sequence  $c_4$ .

Use the value of  $l_q$  in the key to find  $q = |c_4| - l_q$ . Run the function  $\text{posn}_{\text{rotate}}(q) = s_q$ . Use  $s_q$  and  $l_q$  to cut out from  $c$  a sequence  $e(r_q)$  of length  $l_q$  starting at position  $s_q$ , containing a t-encoding of  $r_q$ , leaving a sequence  $c_3$ . t-decode  $e(r_q)$  to find the number of positions  $r_q$  by which  $c_2$  was circularly rotated to the right during encoding. Rotate  $c_3$  circularly by  $r_q$  positions to the left.  
The result is  $c_2$ .

FIG.4

B

FIG. 4

B

5/6

Use the value  $r$  in the key to find  $l = |c_2| - r$ , where  $|c_2|$  is the length of the sequence  $c_2$ .

Find  $\text{posn}_n(l) = s$ , and use  $s$ ,  $r$  and the table  $t$  to find  $n$ , as follows.

Cut out the sequence starting at  $s$  of length  $r$  from  $c_2$  yielding a padded  $t$ -encoded representation  $e(n)$  of  $n$ , and leaving a sequence  $c_1 = \langle q_1, p_{h(1)}, q_2, p_{h(2)}, \dots, q_n, p_{h(n)}, q_{(n+1)} \rangle$ .

$t$ -decode  $e(n)$  and  $e(u)$  to find  $n$  and  $u$  respectively.

Run lengths  $(n, k, u) = \langle l_1, l_2, \dots, l_{(n+1)} \rangle$

C

FIG.5

FIG. 5

C

6/6

Use  $\langle l_1, l_2, \dots, l_{(n+1)} \rangle$  to cut out  $q_1, q_2, \dots, q_{(n+1)}$  from  $c_1$ .

The remaining sequence is  
 $\langle p_{h(1)}, p_{h(2)}, \dots, p_{h(n)} \rangle$

T-decode each of  $q_1, q_2, \dots, q_n$   
 ignoring any symbols not in T.

Result is  $\langle h(1), h(2), \dots, h(n) \rangle$ ,  
 a representation of the  
 permutation h.

Apply the inverse of h to  
 $\langle p_{h(1)}, p_{h(2)}, \dots, p_{h(n)} \rangle$ , yielding  
 the plaintext sequence  $p = \langle p_1, \dots, p_n \rangle$ .

Output the decrypted plaintext p.

FIG.6

TOP SECRET-00000000